

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-307603

(P2000-307603A)

(43) 公開日 平成12年11月2日 (2000.11.2)

(51) Int.Cl.<sup>7</sup>

識別記号

F I

フォーマット (参考)

H 0 4 L 12/28

H 0 4 L 11/00

3 1 0 D 5 K 0 3 0

12/24

11/08

5 K 0 3 3

12/26

審査請求 未請求 請求項の数27 O L (全 22 頁)

(21) 出願番号 特願平11-117197

(22) 出願日 平成11年4月23日 (1999.4.23)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 佐々木 雄飛

神奈川県横浜市港北区綱島東四丁目3番1

号 松下通信工業株式会社内

(72) 発明者 篠原 利章

神奈川県横浜市港北区綱島東四丁目3番1

号 松下通信工業株式会社内

(74) 代理人 100082692

弁理士 蔵合 正博

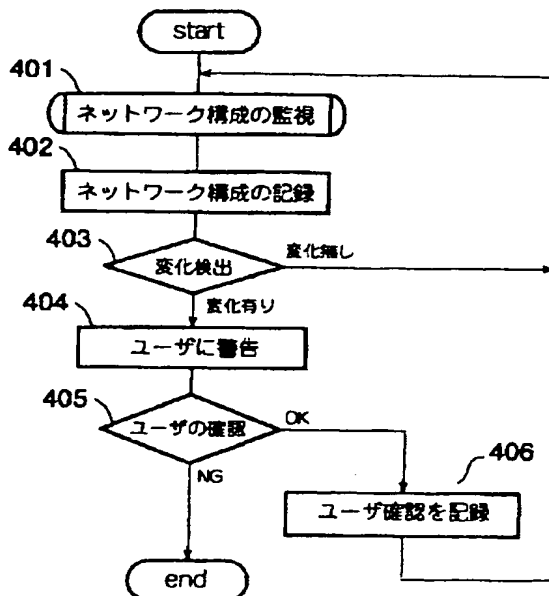
最終頁に続く

(54) 【発明の名称】 ネットワーク監視方法および装置

(57) 【要約】

【課題】 IEEE1394ネットワークに代表される活線接続可能なネットワークにおいて、ネットワークに不正に接続された機器を発見することでセキュリティを保つことを目的とする。

【解決手段】 ネットワークトポロジを監視、記録することまたは伝送遅延の変化を監視、記録することでトポロジの変化からネットワークに追加、削除された機器を発見し、機器固有の情報またはバスリセット前情報で機器の認証を行なう。



## 【特許請求の範囲】

【請求項1】 ネットワーク構成を知る機能を有する機器に問い合わせることによってネットワーク構成を観察し、記録し、観測結果と以前の観測結果の記録との差分を抽出することによってネットワーク構成の変化を認識し、ネットワークに不正な機器が接続されるのを監視するネットワーク監視方法。

【請求項2】 ネットワーク構成を知る機能を有する機器に問い合わせることによってネットワーク構成を検出するネットワーク構成検出部と、検出したネットワーク構成を記録するネットワーク構成記録部と、観測結果と以前の観測結果の記録とを比較するネットワーク構成比較部と、ユーザに警告を示す表示部とを具備することを特徴とするネットワーク監視装置。

【請求項3】 各機器に接続状態を問い合わせることによってネットワーク構成を観察し、記録し、観測結果と以前の観測結果の記録との差分を抽出することによってネットワーク構成の変化を認識するネットワーク監視方法。

【請求項4】 各機器に接続状態を問い合わせることによってネットワーク構成を検出するネットワーク構成検出部と、検出したネットワーク構成を記録するネットワーク構成記録部と、観測結果と以前の観測結果の記録とを比較するネットワーク構成比較部と、ユーザに警告を示す表示部とを具備することを特徴とするネットワークネットワーク監視装置。

【請求項5】 請求項1に記載のネットワーク監視方法において、予めセキュアである条件を与え、それをもとにネットワークがセキュアか否かを自動的に判別するネットワーク監視方法。

【請求項6】 請求項2に記載のネットワーク監視装置において、予めセキュアである条件を与えておく許容ネットワーク構成記録部と、それをもとにネットワークがセキュアか否かを自動的に判別する判断部と、変化をユーザに警告する警告発生部とを具備することを特徴とするネットワーク監視装置。

【請求項7】 請求項3に記載のネットワーク監視方法において、予めセキュアである条件を与え、それをもとにネットワークがセキュアか否かを自動的に判別するネットワーク監視方法。

【請求項8】 請求項4に記載のネットワーク監視装置において、予めセキュアである条件を与えておく許容ネットワーク構成記録部と、それをもとにネットワークがセキュアか否かを自動的に判別する判断部と、変化をユーザに警告する警告発生部とを具備することを特徴とするネットワーク監視装置。

【請求項9】 ネットワーク構成のリセット信号を検出し、ネットワーク構成を知る機能を有する機器に問い合わせることによってネットワーク構成を観察し、記録し、リセット以前とリセット以後の記録との差分を抽出することによってネットワーク構成の変化を認識するネットワーク監視

方法。

【請求項10】 ネットワーク構成のリセット信号を検出するリセット検出部と、ネットワーク構成を知る機能のある機器に問い合わせることによってネットワーク構成を検出するネットワーク構成検出部と、検出したネットワーク構成を記録するネットワーク構成記録部と、観測結果と以前の観測結果の記録とを比較するネットワーク構成比較部と、ユーザに警告を示す表示部とを具備することを特徴とするネットワーク監視装置。

【請求項11】 ネットワーク構成のリセット信号後に発生するネットワーク上の機器の識別信号を受信することによってネットワーク構成を観察し、記録し、リセット以前とリセット以後の記録との差分を抽出することによってネットワーク構成の変化を認識するネットワーク監視方法。

【請求項12】 ネットワーク構成のリセット信号を検出するリセット検出部と、リセット後に発生するネットワーク上の機器の識別信号を受信することによってネットワーク構成を検出するネットワーク構成検出部と、検出したネットワーク構成を記録するネットワーク構成記録部と、観測結果と以前の観測結果の記録とを比較するネットワーク構成比較部と、ユーザに警告を示す表示部とを具備することを特徴とするネットワーク監視装置。

【請求項13】 請求項9に記載のネットワーク監視方法において、予めセキュアである条件を与え、それをもとにネットワークがセキュアか否かを自動的に判別するネットワーク監視方法。

【請求項14】 請求項10に記載のネットワーク監視装置において、予めセキュアである条件を与えておく許容ネットワーク構成記録部と、それをもとにネットワークがセキュアか否かを自動的に判別する判断部と、変化をユーザに警告する警告発生部とを具備することを特徴とするネットワーク監視装置。

【請求項15】 請求項11に記載のネットワーク監視方法において、予めセキュアである条件を与え、それをもとにネットワークがセキュアか否かを自動的に判別するネットワーク監視方法。

【請求項16】 請求項12に記載のネットワーク監視装置において、予めセキュアである条件を与えておく許容ネットワーク構成記録部と、それをもとにネットワークがセキュアか否かを自動的に判別する判断部と、変化をユーザに警告する警告発生部とを具備することを特徴とするネットワーク監視装置。

【請求項17】 複数の手段でネットワーク構成を検出し、各手段から得られるネットワーク構成に矛盾が無いが判定するネットワーク監視方法。

【請求項18】 複数の手段でネットワーク構成を検出するネットワーク構成検出部または複数のネットワーク構成検出部と、検出されたネットワーク構成を記録する記録部と、検出されたネットワーク構成に矛盾がないか調べる比較部とを具備することを特徴とするネットワー

ク監視装置。

【請求項19】 自らネットワーク構成を知り、管理する能力を持ち、ネットワークを管理するマネージャとなり、マネージャになれなかった場合、監視者または上位のネットワーク監視装置に警告を発するネットワーク監視方法。

【請求項20】 自らアイソクロナス転送とそのリソースを管理する能力を持ち、アイソクロナス転送を管理するマネージャとなり、マネージャになれなかった場合、監視者または上位のネットワーク監視装置に警告を発するネットワーク監視方法。

【請求項21】 機器間の伝送遅延を観測し、記録し、観測結果と以前の観測結果の記録との差分を判定し、伝送遅延の変化を認識することでネットワーク構成の変化を認識するネットワーク監視方法。

【請求項22】 機器間の伝送遅延を観測する伝送遅延検出部と、伝送遅延を記録する記録部と、観測結果と以前の観測結果の記録との差分を判定し、検出条件と比較し伝送遅延の変化を検出する変化検出部と、変化をユーザに警告する警告発生部とを具備することを特徴とするネットワーク監視装置。

【請求項23】 伝送遅延検出の条件を設定、記録する検出条件記録部と、伝送遅延測定用のパケットを送出するパケット送信部と、そのackを受信するパケット受信部と、伝送遅延を記録する記録部と、観測結果と以前の観測結果の記録との差分を判定し、検出条件と比較し伝送遅延の変化を検出する変化検出部と、変化をユーザに警告する警告発生部とを具備することを特徴とするネットワーク監視装置。

【請求項24】 ネットワーク上のデータパケットとそれに対するackを監視するパケット監視部と、伝送遅延を記録する記録部と、観測結果と以前の観測結果の記録との差分を判定し、検出条件と比較し伝送遅延の変化を検出する変化検出部と、変化をユーザに警告する警告発生部とを具備することを特徴とするネットワーク監視装置。

【請求項25】 複数の機器からなるネットワークシステムで、ネットワーク構成をリセットする信号の前に予め情報を交換しておき、リセット後に予め交換しておいた情報に基づく認証を行なうことで、リセット以前から存在した機器と新たに追加された機器および削除された機器を認識するネットワーク監視方法。

【請求項26】 ネットワーク構成をリセットする信号の前に交換する情報を生成する鍵生成部と、リセット前情報を記録しておく記録部と、リセットを検出するリセット検出部と、予め交換しておいた情報に基づきリセット後に認証を行なう機器認証処理部とを具備することを特徴とするネットワーク監視装置。

【請求項27】 請求項1から26に記載のネットワーク監視方法およびネットワーク監視装置のいずれかを具

備するネットワーク監視システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ネットワークのセキュリティに係り、特にIEEE1394に代表される活線接続可能なネットワークにおける機器の不正接続に対するセキュリティに関する。

【0002】

【従来の技術】 IEEE1394は、シンプルな構成と高いパフォーマンスにより家庭内LANなど今後の様々な機器間接続手段として期待されている。100Mbps以上の転送速度、Isochronousと呼ばれるマルチメディアデータ転送に適した転送方式、機器の接続を自動的に認識することでネットワークの稼働中に機器を追加、削除が可能な活線接続機能を備え、トゥリー型のネットワークを構成し、広い用途に活用することが可能である。

【0003】 用途のひとつにカメラを用いた監視システムを構成することが考えられる。これは、高速な転送速度のために多量の映像等のデータを伝送することが可能になるためである。従来の監視システムの場合、監視に必要な数のアナログ出力カメラとそれと同数のビデオキャプチャボード等のA/D変換機構を必要とし、また、カメラとビデオキャプチャボードとの接続に一本のケーブルを必要とし、カメラ台数と同じ本数のケーブルを引き回す必要があった。

【0004】 しかし、IEEE1394などの活線接続が可能なネットワークを利用した監視システムの場合、監視に必要な数のデジタル出力カメラに対し、ネットワーク監視装置として受信、記録のためのパソコンを最低ひとつ接続するだけで済み、またトゥリー型のネットワークを構成することにより、少ないケーブル本数で監視システムを構成することが可能である。

【0005】

【発明が解決しようとする課題】 活線接続が可能なネットワークでは、ネットワークに簡単に機器を接続することができる。これは便利な機能である反面、監視システムなどのセキュリティの必要とされるネットワークにおいては部外者に不正に機器を接続された場合、ネットワーク上の情報の盗聴、改ざん、不正なパケットの発信など重大な問題を引き起こす可能性がある。このためIEEE1394などの活線接続が可能なネットワークにおいては、ネットワークに接続してくる機器を監視し、それが不正な機器であるか否かを判別し、不正な機器の接続を防止することでネットワーク自体をセキュアに保つことが望ましい。

【0006】 そこで本発明では、ネットワークへの機器の追加、削除およびネットワーク構成の変化を監視し、ネットワークへの不正な機器の接続を発見することのできるネットワーク監視方法および装置を提供することを

目的とする。

【0007】

【課題を解決するための手段】原理的には、ネットワークのノードとなる機器がポート別に接続状態を把握可能であれば、ネットワーク構成を得ることができる。IEEE1394ネットワークでは、ひとつの機器が複数のポートを持つが、接続はポート毎に認識が可能である。これを利用するとネットワークの構成を知ることができる。

【0008】活線接続可能なネットワークにおいては、機器をネットワークに接続、ネットワークから削除する際に、ネットワークを初期化し、機器のIDを決定する等の理由でネットワークにリセットを掛ける必要がある。リセット後には各機器の能力、状態を交換し、各機器のIDを決定しネットワーク構成を明らかにする。これらによりネットワーク構成を得ることができ、またネットワーク構成の変化を検出することができる。

【0009】IEEE1394ネットワークでは、新しい機器が接続されたりすでに接続されている機器が削除されたりすると、バスリセットがかかり、ネットワーク構成の認識を始める。IEEE1394ネットワークのノードは、階層型の親子関係を持つ。バスリセット後は最初に親子関係を決定する。接続されたポートをひとつしか持たないノードはリーフと呼ばれ、自ら子ノードとなろうとし、接続されたポートに接続された隣接するノードに、自分は子ノードとなる旨伝達する。伝達を受けたノードは親ノードとなる。親ノードとなったノードは、ネットワークがトゥリー型であることが保証されているため、遅かれ早かれ(A)接続されているノードすべてが子ノードになるか、あるいは(B)ひとつの接続されているノードを除いたすべての接続されているノードが子ノードとなる。(A)の状況になった場合、そのノードはルートとなり、親子関係の構築は終了する。

(B)の状況になった場合、そのノードは残された接続されたポートに接続された隣接するノードに自分は子ノードとなる旨伝達し、以後再帰的にルートが決定されるまで繰り返す。

【0010】親子関係が決定すると、親子の序列上決められた順番に自己識別バケットと呼ばれるバケットをブロードキャストし、各ノードのIDを決定してゆく。全ノードのIDが決定すると、ネットワークの構築の終了であり、以後は普通にデータ伝送が行なわれる。自己識別バケットには、各ノードのポート毎の接続状態が記録されている。このバケットを、トポロジマップレジスタと呼ばれるレジスタを持った機器が収集し、ネットワーク構成を明らかにし、トポロジマップレジスタに格納する。ネットワーク上の機器は、トポロジマップレジスタを見ることによりネットワーク構成を知ることができる。また、ネットワーク監視装置が自ら自己識別バケットを収集し、ネットワーク構成を知ることでもある。

【0011】以上述べたようにIEEE1394では、ネットワーク構成を得ることが容易であり、ネットワーク構成の変化を監視することで不正な機器の接続が行なわれた可能性を検出することが可能になる。活線接続可能なネットワークにおいて、ネットワークを管理する機器は必ずしも一意に決定されるとは限らず、何らかの交渉を通じて管理者が決定することがある。この時、管理者を監視し、問題のある機器が管理者になることを防ぐ必要がある。

【0012】IEEE1394では、バスマネージャはトポロジマップを持つことが保証されているが、バスマネージャは能力さえあれば成ることが可能なため、どの機器がバスマネージャになるかも監視する。また、バスマネージャを決定するのはアイソクロナスマネージャであるため、どの機器がアイソクロナスマネージャになるかも監視する。また、活線接続であることを利用し、自己識別バケットを偽る、あるいは出力しないノードが正常なノードの間に不正に接続される可能性がある。そこで伝送遅延を測定、記録し、変化を検出することで、不正なノードを検出する。また、ネットワーク構成が変化した際のリセットの前に適当な情報を共有しておき、リセット後にその情報を用いた認証を行なうことで、機器がリセット以前から存在したかどうかを検出することが可能となる。これらに通常の認証を加えて機器の正当性を確認することで、さらにネットワークのセキュアを高めることができる。

【0013】

【発明の実施の形態】請求項1に記載のネットワーク監視方法は、ネットワーク構成を知る機能を有する機器に問い合わせることでネットワーク構成を観察し、記録し、観測結果と以前の観測結果の記録との差分を抽出することでネットワーク構成の変化を認識し、ネットワークに不正な機器が接続されるのを監視することを特徴とし、特別な手段を必要とせず、ネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出することで、ネットワークをセキュアに保つことができるという作用を有する。

【0014】請求項2に記載のネットワーク監視装置は、ネットワーク構成を知る機能を有する機器に問い合わせることでネットワーク構成を検出するネットワーク構成検出部と、検出したネットワーク構成を記録するネットワーク構成記録部と、観測結果と以前の観測結果の記録とを比較するネットワーク構成比較部と、ユーザに警告を示す表示部とを具備することを特徴とし、監視機器にネットワーク構成検出能力を必要とせずにネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出することができるという作用を有する。

【0015】請求項3に記載のネットワーク監視方法は各機器に接続状態を問い合わせることでネットワーク構

成を観察し、記録し、観測結果と以前の観測結果の記録との差分を抽出することでネットワーク構成の変化を認識することを特徴とし、ネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出することができるという作用を有する。

【0016】請求項4に記載のネットワーク監視装置は各機器に接続状態を問い合わせることでネットワーク構成を検出するネットワーク構成検出部と、検出したネットワーク構成を記録するネットワーク構成記録部と、観測結果と以前の観測結果の記録とを比較するネットワーク構成比較部と、ユーザに警告を示す表示部とを具備することを特徴とし、ネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出することができるという作用を有する。

【0017】請求項5に記載のネットワーク監視方法は、請求項1に記載のネットワーク監視方法において、予めセキュアである条件を与え、それをもとにネットワークがセキュアか否かを自動的に判別することを特徴とし、特別な手段を必要とせず、ネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出し、与えられた条件に因ってネットワークがセキュアか否かを自動的に判断することができるという作用を有する。

【0018】請求項6に記載のネットワーク監視装置は、請求項2に記載のネットワーク監視装置において、予めセキュアである条件を与えておく許容ネットワーク構成記録部と、それをもとにネットワークがセキュアか否かを自動的に判別する判断部と、変化をユーザに警告する警告発生部とを具備することを特徴とし、特別な手段を必要とせず、ネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出し、与えられた条件に因ってネットワークがセキュアか否かを自動的に判断することができるという作用を有する。

【0019】請求項7に記載のネットワーク監視方法は、請求項3に記載のネットワーク監視方法において、予めセキュアである条件を与え、それをもとにネットワークがセキュアか否かを自動的に判別することを特徴とし、ネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出し、与えられた条件に因ってネットワークがセキュアか否かを自動的に判断することができるという作用を有する。

【0020】請求項8に記載のネットワーク監視装置は、請求項4に記載のネットワーク監視装置において、予めセキュアである条件を与えておく許容ネットワーク構成記録部と、それをもとにネットワークがセキュアか否かを自動的に判別する判断部と、変化をユーザに警告する警告発生部とを具備することを特徴とし、ネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出し、与えられた条

件に因ってネットワークがセキュアか否かを自動的に判断することができるという作用を有する。

【0021】請求項9に記載のネットワーク監視方法は、ネットワーク構成のリセット信号を検出し、ネットワーク構成を知る機能のある機器に問い合わせることでネットワーク構成を観察し、記録し、リセット以前とリセット以後の記録との差分を抽出することでネットワーク構成の変化を認識することを特徴とし、特別な手段を必要とせず、最小の手順でネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出することができるという作用を有する。

【0022】請求項10に記載のネットワーク監視装置はネットワーク構成のリセット信号を検出するリセット検出部と、ネットワーク構成を知る機能のある機器に問い合わせることでネットワーク構成を検出するネットワーク構成検出部と、検出したネットワーク構成を記録するネットワーク構成記録部と、観測結果と以前の観測結果の記録とを比較するネットワーク構成比較部と、ユーザに警告を示す表示部とを具備することを特徴とし、特別な手段を必要とせず、最小の手順でネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出することができるという作用を有する。

【0023】請求項11に記載のネットワーク監視方法は、ネットワーク構成のリセット信号後に発生するネットワーク上の機器の識別信号を受信することでネットワーク構成を観察し、記録し、リセット以前とリセット以後の記録との差分を抽出することでネットワーク構成の変化を認識することを特徴とし、特別な手段を必要とせず、またトラフィックを増加させることなく、最小の手順でネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出することができるという作用を有する。

【0024】請求項12に記載のネットワーク監視装置は、ネットワーク構成のリセット信号を検出するリセット検出部と、リセット後に発生するネットワーク上の機器の識別信号を受信することでネットワーク構成を検出するネットワーク構成検出部と、検出したネットワーク構成を記録するネットワーク構成記録部と、観測結果と以前の観測結果の記録とを比較するネットワーク構成比較部と、ユーザに警告を示す表示部とを具備することを特徴とし、特別な手段を必要とせず、またトラフィックを増加させることなく、最小の手順でネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出することができるという作用を有する。

【0025】請求項13に記載のネットワーク監視方法は、請求項9に記載のネットワーク監視方法において、予めセキュアである条件を与え、それをもとにネットワ

ークがセキュアか否かを自動的に判別することを特徴とし、特別な手段を必要とせず、最小の手順でネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出し、与えられた条件に因ってネットワークがセキュアか否かを自動的に判断することができるという作用を有する。

【0026】請求項14に記載のネットワーク監視装置は、請求項10に記載のネットワークネットワーク監視装置において、予めセキュアである条件を与えておく許容ネットワーク構成記録部と、それをもとにネットワークがセキュアか否かを自動的に判別する判断部と、変化をユーザに警告する警告発生部とを具備することを特徴とし、特別な手段を必要とせず、最小の手順でネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出し、与えられた条件に因ってネットワークがセキュアか否かを自動的に判断することができるという作用を有する。

【0027】請求項15に記載のネットワーク監視方法は、請求項11に記載のネットワーク監視方法において、予めセキュアである条件を与え、それをもとにネットワークがセキュアか否かを自動的に判別することを特徴とし、特別な手段を必要とせず、またトラフィックを増加させることなく、最小の手順でネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出し、与えられた条件に因ってネットワークがセキュアか否かを自動的に判断することができるという作用を有する。

【0028】請求項16に記載のネットワーク監視装置は、請求項12に記載のネットワークネットワーク監視装置において、予めセキュアである条件を与えておく許容ネットワーク構成記録部と、それをもとにネットワークがセキュアか否かを自動的に判別する判断部と、変化をユーザに警告する警告発生部とを具備することを特徴とし、特別な手段を必要とせず、またトラフィックを増加させることなく、最小の手順でネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出し、与えられた条件に因ってネットワークがセキュアか否かを自動的に判断することができるという作用を有する。

【0029】請求項17に記載のネットワーク監視方法は、複数の手段でネットワーク構成を検出し、各手段から得られるネットワーク構成に矛盾が無いかが判定することを特徴とし、フォールトトレランスを維持することができ、また、不正なトポロジマップを検出することでネットワークに不正な機器の接続された可能性を検出することができるという作用を有する。

【0030】請求項18に記載のネットワーク監視装置は、複数の手段でネットワーク構成を検出するネットワーク構成検出部または複数のネットワーク構成検出部と、検出されたネットワーク構成を記録する記録部と、

検出されたネットワーク構成に矛盾がないか調べる比較部とを具備することを特徴とし、ネットワーク構成獲得手段を複数持つことでフォールトトレランスを維持することができ、また、不正なネットワーク構成を報告したネットワーク構成獲得手段を検出することでネットワークに不正な機器の接続された可能性を検出することができるという作用を有する。

【0031】請求項19に記載のネットワーク監視方法は、自らネットワーク構成を知り、管理する能力を持ち、ネットワークを管理するマネージャとなり、マネージャになれなかった場合、監視者または上位のネットワーク監視装置に警告を発することを特徴とし、ネットワークを管理するマネージャの乗っ取りを防止するという作用を有する。

【0032】請求項20に記載のネットワーク監視方法は、自らアイソクロナス転送とそのリソースを管理する能力を持ち、アイソクロナス転送を管理するマネージャとなり、監視者または上位のネットワーク監視装置に警告を発することを特徴とし、アイソクロナス転送を管理するマネージャの乗っ取りを防止するという作用を有する。

【0033】請求項21に記載のネットワーク監視方法は、機器間の伝送遅延を観測し、記録し、観測結果と以前の観測結果の記録との差分を判定し伝送遅延の変化を認識することでネットワーク構成の変化を認識することを特徴とし、ネットワークに不正な機器の接続された可能性を検出することができるという作用を有する。

【0034】請求項22に記載のネットワーク監視装置は、機器間の伝送遅延を観測する伝送遅延検出部と、伝送遅延を記録する記録部と、観測結果と以前の観測結果の記録との差分を判定し、検出条件と比較し伝送遅延の変化を検出する変化検出部と、変化をユーザに警告する警告発生部とを具備することを特徴とし、ネットワークにノードとして振舞わない不正な機器の接続された可能性を検出することができるという作用を有する。

【0035】請求項23に記載のネットワーク監視装置は、伝送遅延検出の条件を設定、記録する検出条件記録部と、伝送遅延測定用のパケットを送出するパケット送信部と、そのackを受信するパケット受信部と、伝送遅延を記録する記録部と、観測結果と以前の観測結果の記録との差分を判定し、検出条件と比較し伝送遅延の変化を検出する変化検出部と、変化をユーザに警告する警告発生部とを具備することを特徴とし、ネットワークにノードとして振舞わない不正な機器の接続された可能性を検出することができるという作用を有する。

【0036】請求項24に記載のネットワーク監視装置は、ネットワーク上のデータパケットとそれに対するackを監視するパケット監視部と、伝送遅延を記録する記録部と、観測結果と以前の観測結果の記録との差分を判定し、検出条件と比較し伝送遅延の変化を検出する変

化検出部と、変化をユーザに警告する警告発生部とを具備することを特徴とし、トラフィックを増加させることなく、ネットワークにノードとして振舞わない不正な機器の接続された可能性を検出することができるという作用を有する。

【0037】請求項25に記載のネットワーク監視方法は、複数の機器からなるネットワークシステムで、ネットワーク構成をリセットする信号の前に予め情報を交換しておき、リセット後に予め交換しておいた情報に基づく認証を行なうことで、リセット以前から存在した機器と新たに追加された機器および削除された機器を認識することを特徴とし、リセット以前から存在する機器を識別し、ネットワークに新たに接続された不正な機器を発見することができるという作用を有する。

【0038】請求項26に記載のネットワーク監視装置は、ネットワーク構成をリセットする信号の前に交換する情報を生成する鍵生成部と、リセット前情報を記録しておく記録部と、リセットを検出するリセット検出部と、予め交換しておいた情報に基づきバスリセット後に認証を行なう機器認証処理部とを具備することを特徴とし、リセット以前から存在する機器を識別し、ネットワークに新たに接続された不正な機器を発見することができるという作用を有する。

【0039】請求項27に記載のネットワーク監視システムは、請求項1から26に記載のネットワーク監視方法およびネットワーク監視装置のいずれかを具備することを特徴とし、ネットワークをセキュアに保つことで安全にネットワーク上でデータの送受信をすることが可能であるという作用を有する。

【0040】以下、添付図面の図1から20に基づき、本発明の実施の形態を詳細に説明する。なお、ここでは活線接続可能なネットワークとしてIEEE1394ネットワークの場合を想定して説明している。また、以下の説明において、ネットワーク構成とは、どの機器の何番のポートにどの機器の何番のポートが接続されているかという情報であり、ネットワーク構成を検出するとは、ここではネットワーク内のノードとアークの関係を把握することを指す。ネットワーク構成の検出の手段としては、バスマネージャなどの物理層でトポロジマップを持つ機器に問い合わせを行なう、機器に接続状態を問い合わせる、自らバスマネージャになる、等の方法がある。

【0041】トポロジマップを持つ機器に問い合わせる方法は、ネットワーク監視装置に特別な能力が無くともネットワーク構成を知ることができるという作用がある。機器に接続状態を問い合わせる方法は、物理層に直接アクセスすること無しにネットワーク構成を知ることができ、またネットワーク構成情報以外の情報も同時に扱うことができるという作用がある。ネットワーク監視装置自らがバスマネージャになる場合、自分以外の機器

がバスマネージャに決定したか、あるいは自分以外の機器がバスマネージャに立候補したかという情報をセキュリティの判断に用いることができる。この情報を得ることは、バスマネージャになりすまそうとする不正な機器を発見することができるという作用を有する。自らバスマネージャにならない場合、バスマネージャを決定するアイソクロナスマネージャに自らがなっても良い。この時、自分以外の機器がアイソクロナスマネージャに決定したか、あるいは自分以外の機器がアイソクロナスマネージャに立候補したか、あるいは自分がバスマネージャに決定した機器以外の機器がバスマネージャに立候補したかという情報をセキュリティの判断に用いることができる。この情報を得ることは、アイソクロナスマネージャまたはバスマネージャになりすまそうとする不正な機器を発見することができるという作用を有する。

【0042】セキュアなネットワーク構成の条件としては、セキュアなネットワーク構成のリスト、ネットワークに接続が許容されている機器と接続位置のリスト、許容されている機器の組、許容されている機器間のアークのトポロジ、許されるネットワーク構成変化のリスト、あるいはこれらを論理的に記述した式等、あるいはこれらの組合せが用いられる。

【0043】(実施の形態1)図1は本発明の実施の形態1におけるネットワーク監視方法を説明する図である。図1において、301a~301dはネットワークを構成するカメラ、308はネットワーク監視装置、311はネットワーク監視装置に登録されている機器およびネットワークの登録リストである。

【0044】次に、図1を参照して本発明の実施の形態1におけるネットワーク監視方法を説明する。ネットワーク監視装置308は、ネットワーク構成を獲得する能力があり、また、ネットワーク機器についての固有な情報を得る手段を持っている。ここでは情報として機器のIDとして製造元および製造番号を用いる場合を説明する。ネットワーク監視装置308は、許容されるネットワーク機器およびネットワーク構成に登録する登録リスト311を持つ。登録リスト311の内容は、事前に登録されても良いし、ネットワーク監視装置308が監視結果を記録して更新してもよい。ここでは、ネットワーク監視装置308、カメラ301a、カメラ301b、カメラ301cからなるネットワークが登録リスト311に登録されている。現在のネットワーク上の機器およびネットワーク構成は登録リスト311の内容に合致するために許容される。

【0045】ここでカメラ301dをネットワークに接続するとする。その場合、ネットワーク上のネットワーク機器およびネットワーク構成が変化する。ネットワーク監視装置308は、ネットワーク機器の情報およびネットワーク構成を獲得し、それを登録リスト311と比較する。ネットワーク機器の情報およびネットワーク構

成が登録リスト311の内容と合致しない場合、ネットワーク監視装置308は警告を発する。

【0046】本発明の実施の形態1におけるネットワーク監視方法を以上のように構成することにより、ネットワーク機器の情報およびネットワーク構成を利用し、ネットワークに不正な機器が接続された可能性を検出できるネットワーク監視方法を実現することができる。

【0047】(実施の形態2)図2は本発明の実施の形態2におけるネットワーク監視方法の流れ図である。図2において、401はネットワーク構成の監視フェイズ、402はネットワーク構成の記録フェイズ、403はネットワーク構成の変化検出フェイズ、404はユーザに警告を行なうフェイズ、405はユーザの確認を受けるフェイズ、406はユーザの確認を受けたことを記録するフェイズである。

【0048】次に、図2を参照して本発明の実施の形態2におけるネットワーク監視方法を説明する。監視者は設定された時刻にネットワーク構成を検出する(401)。検出時刻については、バスリセット直後、一定時間間隔、ランダム時間間隔、トラフィックの少ない時間、特定のイベントの直前または直後、ユーザの指示した時刻、常時、等の手段がある。検出されたネットワーク構成は記録される(402)。検出されたネットワーク構成は、過去に記録されたネットワーク構成または特に設定されたネットワーク構成と比較される(403)。比較の結果、変化が認められなかった場合には401に戻り、次のネットワーク構成検出まで待機する。比較の結果変化が認められた場合、ユーザに警告を行なう(404)。警告を受けたユーザは現在のネットワーク構成がセキュアであるか否かを判断する。ユーザがセキュアであると判断した場合、その旨を記録し(406)、401に戻り、次のネットワーク構成検出まで待機する。

【0049】なお、ユーザへの警告404は、警告音や音声を利用または表示と警告音、音声を併用した警告を行なってもよい。また、警告理由およびその判断材料となった情報を提示しても良い。また、ネットワークの運用を停止する、ネットワークの接続を強制切断する、等の対策を警告と共に行なっても良い。

【0050】本発明の実施の形態2におけるネットワーク監視方法を以上のように構成することにより、ネットワーク構成の変化を検出し、ネットワークに不正な機器の接続された可能性を検出できるネットワーク監視方法を実現することができる。

【0051】(実施の形態3)図3は本発明の実施の形態3におけるネットワーク監視装置の構成を示すブロック図である。図3において、101はネットワーク、102はネットワーク構成を検出するネットワーク構成検出部、103はネットワーク構成を記録するネットワーク構成記録部、104はネットワーク構成の変化を検出

するネットワーク構成変化検出部、105はネットワーク構成の変化を表示する表示部であり、110はユーザからの入力を受け付ける入力部である。

【0052】次に、図3を参照して本発明の実施の形態3におけるネットワーク監視装置の動作を説明する。最初に、ネットワークがセキュアな状態において、ネットワーク構成検出部102は、現在のセキュアなネットワーク構成を検出し、ネットワーク構成記録部103は、そのネットワーク構成をそれがセキュアであるというセキュリティ情報を付加して記録する。次に、ネットワーク構成検出部102は、ネットワーク構成を検出する。ネットワーク構成変化検出部104は、現在のネットワーク構成と記録されているセキュアなネットワーク構成とを比較し、ネットワーク構成に変化があった場合それを検出し、表示部105に変化を出力する。表示部105は、ネットワーク構成変化検出部104からの入力を受けて、それをユーザに対し表示する。また、ネットワーク構成の変化が検出された場合、ネットワーク構成記録部103は、新たなネットワーク構成を、セキュアではないというセキュリティ情報を付加して記録する。ユーザは、表示部110を見てそれがセキュアなネットワーク構成であるかどうかを確認し、もしそのネットワーク構成がセキュアであった場合、その旨を入力部110に入力する。ネットワーク構成記録部103は、入力部110からの入力を受け、新たなネットワーク構成に付加されたセキュリティ情報を、セキュアであると書き換える。

【0053】なお、表示部110の代わりに、警告音や音声を利用または表示と警告音、音声を併用した警告を行なってもよい。また、警告理由およびその判断材料となった情報を提示しても良い。また、ネットワークの運用を停止する、ネットワークの接続を強制切断する、等の対策を警告とともに行なっても良い。

【0054】本発明の実施の形態3におけるネットワーク監視装置を以上のように構成することにより、ネットワーク構成の変化を検出し、ネットワークに不正な機器の接続された可能性を検出できるネットワーク監視装置を実現することができる。

【0055】(実施の形態4)図4は本発明の実施の形態4におけるネットワーク監視方法の流れ図であり、図2に示す構成部の符号と同一の符号を有する構成部は同様のため、説明を省略する。図4において、407は現在のネットワーク構成がセキュアであるという条件を新たに登録するフェイズ、408は登録されているセキュアなネットワーク構成の条件と現在のネットワークとを比較するフェイズ、409は比較結果、現在のネットワーク構成がセキュアか否かを判断するフェイズ、410はセキュアなネットワーク構成の条件を設定するフェイズである。

【0056】次に、図4を参照して本発明の実施の形態



4におけるネットワーク監視方法を説明する。最初にネットワークがセキュアか否かを判断するための条件を設定する(410)。監視者は設定された時刻にネットワーク構成を検出する(401)。検出時刻については、バスリセット直後、一定時間間隔、ランダム時間間隔、トラフィックの少ない時間、特定のイベントの直前または直後、ユーザの指示した時刻、常時、等の手段がある。検出されたネットワーク構成は記録される(402)。検出されたネットワーク構成は、過去に記録されたネットワーク構成または特に設定されたネットワーク構成と比較される(403)。比較の結果、変化が認められなかった場合には401に戻り、次のネットワーク構成検出まで待機する。比較の結果変化が認められた場合、検出された現在のネットワーク構成をセキュアなネットワーク構成の条件と比較し(408)、条件に合致するか否かを判断する(409)。現在のネットワーク構成がセキュアでなネットワーク構成の条件に合致した場合、401に戻り、次のネットワーク構成検出まで待機する。合致しなかった場合、ユーザに警告を行なう(404)。警告を受けたユーザは現在のネットワーク構成がセキュアであるか否かを判断する。ユーザがセキュアであると判断した場合、現在のネットワーク構成をセキュアなネットワーク構成の条件として新たに登録し(407)、401に戻り次のネットワーク構成検出まで待機する。

【0057】なお、ユーザへの警告404は、警告音や音声を利用または表示と警告音、音声を併用した警告を行なってもよい。また、警告理由およびその判断材料となった情報を提示してもよい。また、ネットワークの運用を停止する、ネットワークの接続を強制切断する、等の対策を警告とともに行なってもよい。

【0058】本発明の実施の形態4におけるネットワーク監視方法を以上のように構成することにより、ネットワーク構成の変化を検出し、ネットワークに不正な機器の接続された可能性を検出することができ、与えられた条件に因ってネットワークがセキュアか否かを自動的に判断するネットワーク監視方法を実現することができる。

【0059】(実施の形態5)図5は本発明の実施の形態5におけるネットワーク監視装置の構成を示すブロック図であり、図3に示す構成部の符号と同一の符号を有する構成部は同様のため、説明を省略する。図5において、106は予めセキュアであるとされたネットワーク構成を記録しておく許容ネットワーク構成記録部、107はネットワーク構成が変化した場合にその新たなネットワーク構成はセキュアであるか否かを判断する判断部、108は変化した新たなネットワークがセキュアではないと判断された場合に警告を発する警告発生部である。

【0060】次に、図5を参照して本発明の実施の形態

5におけるネットワーク監視装置の動作を説明する。最初にユーザは、セキュアであると解っているネットワーク構成を許容ネットワーク構成記録部106に登録する。また、ネットワーク構成検出部102は、現在のセキュアなネットワーク構成を検出し、ネットワーク構成記録部103は、そのネットワーク構成をそれがセキュアであるというセキュリティ情報を付加して記録する。次に、ネットワーク構成検出部102は、ネットワーク構成を検出する。ネットワーク構成変化検出部104は、現在のネットワーク構成と記録されているセキュアなネットワーク構成とを比較し、ネットワーク構成に変化があった場合それを検出し、判断部107に出力する。また、ネットワーク構成の変化が検出された場合、ネットワーク構成記録部103は、新たなネットワーク構成を、セキュアではないというセキュリティ情報を付加して記録する。判断部107は、ネットワーク構成変化検出部104からの入力を受けると、許容ネットワーク構成記録部106に記録されているセキュアと認定されているネットワーク構成と新たなネットワーク構成とを比較する。もし新たなネットワーク構成が、許容ネットワーク構成記録部106に記録されているセキュアと認定されているネットワーク構成に含まれる場合、判断部107は、ネットワーク構成記録部103に記録された新たなネットワーク構成に付加されたセキュリティ情報を、セキュアであると書き換える。この時、判断部107は、変化があったことを警告発生部108に出力してもよい。もし新たなネットワーク構成が、許容ネットワーク構成記録部106に記録されているセキュアと認定されているネットワーク構成に含まれない場合、判断部107は、その旨を警告発生部108に出力する。警告発生部108は、判断部107からの入力を受け、ユーザに対し警告を発する。ユーザは表示部105を見てそれがセキュアなネットワーク構成であるかどうかを確認し、もしそのネットワーク構成がセキュアであった場合、その旨を入力部110に入力する。ネットワーク構成記録部103は入力部110からの入力を受け、新たなネットワーク構成に付加されたセキュリティ情報を、セキュアであると書き換える。また、もしそのネットワーク構成がセキュアであった場合、ユーザは入力部110を介して許容ネットワーク構成記録部に新たなネットワーク構成を追加することもできる。

【0061】なお、警告発生部108は、警告音や音声を利用または表示と警告音、音声を併用した警告を行なってもよい。また、警告理由およびその判断材料となった情報を提示してもよい。また、ネットワークの運用を停止する、ネットワークの接続を強制切断する、等の対策を警告とともに行なってもよい。

【0062】本発明の実施の形態5におけるネットワーク監視方法を以上のように構成することにより、ネットワーク構成の変化を検出し、ネットワークに不正な機器

の接続された可能性を検出することができ、与えられた条件に因ってネットワークがセキュアか否かが自動的に判断するネットワーク監視方法を実現することができる。

【0063】（実施の形態6）図6は本発明の実施の形態6におけるネットワーク監視装置の構成を示すブロック図である。これは図5の構成においてネットワーク構成記録部103とネットワーク構成変化検出部104とを省略した構成である。このような構成にした場合、実施の形態5の場合と比較して、ネットワーク構成が変化しない場合でも判断を行なわねばならず、判断部107の処理が多くなる一方、全体の構成が簡単になる。

【0064】本発明の実施の形態6におけるネットワーク監視装置を以上のように構成することにより、簡易な構成で、ネットワーク構成の変化を検出し、予め与えられた情報を基にネットワークに不正な機器の接続された可能性を自動的に検出できるネットワーク監視装置を実現することができる。

【0065】（実施の形態7）図7は本発明の実施の形態7におけるネットワーク監視方法の流れ図であり、図2に示す構成部の符号と同一の符号を有する構成部は同様のため、説明を省略する。図7において、411はバスリセット監視フェイズであり、412はバスリセットが起こったか否かを判断するフェイズである。

【0066】次に、図7を参照して本発明の実施の形態7におけるネットワーク監視方法を説明する。監視者はバスリセットが発生しているか否かを検出する（411）。バスリセットが発生しない場合は待機する（412）。バスリセットが発生したら、ネットワーク構成を検出する（401）。検出されたネットワーク構成は記録される（402）。検出されたネットワーク構成は、過去に記録されたネットワーク構成または特に設定されたネットワーク構成と比較される（403）。比較の結果変化が認められなかった場合には411に戻り、次のバスリセットが検出されるまで待機する。比較の結果、変化が認められた場合、ユーザに警告を行なう（404）。警告を受けたユーザは現在のネットワーク構成がセキュアであるか否かを判断する。ユーザがセキュアであると判断した場合、その旨を記録し（406）、401に戻り、次のバスリセットが検出されるまで待機する。

【0067】なお、ユーザへの警告404は、警告音や音声を利用または表示と警告音、音声を併用した警告を行なってもよい。また、警告理由およびその判断材料となった情報を提示しても良い。また、ネットワークの運用を停止する、ネットワークの接続を強制切断する、等の対策を警告とともに行なっても良い。

【0068】本発明の実施の形態7におけるネットワーク監視方法を以上のように構成することにより、最小の手順でネットワーク構成の変化を検出することができ、ネットワークに不正な機器の接続された可能性を検出

し、与えられた条件に因ってネットワークがセキュアか否かが自動的に判断するネットワーク監視方法を実現することができる。

【0069】（実施の形態8）図8は本発明の実施の形態8におけるネットワーク監視装置の構成を示すブロック図であり、図3に示す構成部の符号と同一の符号を有する構成部は同様のため、説明を省略する。図8において、109はネットワークのバスリセットを検出するバスリセット検出部である。

【0070】次に、図8を参照して本発明の実施の形態8におけるネットワーク監視装置の動作を説明する。最初に、ネットワークがセキュアな状態において、ネットワーク構成検出部102は、現在のセキュアなネットワーク構成を検出し、ネットワーク構成記録部103は、そのネットワーク構成をそれがセキュアであるというセキュリティ情報を付加して記録する。次に、バスリセット検出部109は、ネットワークのバスリセットを検出すると、その旨をネットワーク構成検出部102に出力する。ネットワーク構成検出部102は、それを受けてバスリセット後のネットワーク構成を検出する。ネットワーク構成変化検出部104は、現在のネットワーク構成と記録されているセキュアなネットワーク構成とを比較し、ネットワーク構成に変化があった場合それを検出し、表示部105に変化を出力する。表示部105は、ネットワーク構成変化検出部104からの入力を受けて、それをユーザに対し表示する。また、ネットワーク構成の変化が検出された場合、ネットワーク構成記録部103は新たなネットワーク構成を、セキュアではないというセキュリティ情報を付加して記録する。ユーザは表示部105を見てそれがセキュアなネットワーク構成であるかどうかを確認し、もしそのネットワーク構成がセキュアであった場合、その旨を入力部110に入力する。ネットワーク構成記録部103は、入力部110からの入力を受け、新たなネットワーク構成に付加されたセキュリティ情報を、セキュアであると書き換える。

【0071】なお、表示部105の代わりに、警告音や音声を利用または表示と警告音、音声を併用した警告を行なってもよい。また、警告理由およびその判断材料となった情報を提示しても良い。また、ネットワークの運用を停止する、ネットワークの接続を強制切断する、等の対策を警告とともに行なっても良い。

【0072】本発明の実施の形態8におけるネットワーク監視装置を以上のように構成することにより、バスリセットにともなうネットワーク構成の変化を最小の手順で検出し、ネットワークに不正な機器の接続された可能性を検出できるネットワーク監視装置を実現することができる。

【0073】（実施の形態9）図9は本発明の実施の形態9におけるネットワーク監視方法の流れ図であり、図4および図7に示す構成部の符号と同一の符号を有する

構成部は同様のため、説明を省略する。

【0074】次に、図9を参照して本発明の実施の形態9におけるネットワーク監視方法を説明する。最初にネットワークがセキュアか否かを判断するための条件を設定する(410)。監視者はバスリセットが発生しているか否かを検出する(411)。バスリセットが発生しない場合は待機する(412)。バスリセットが発生したら、ネットワーク構成を検出する(401)。検出されたネットワーク構成は記録される(402)。検出されたネットワーク構成は、過去に記録されたネットワーク構成または特に設定されたネットワーク構成と比較される(403)。比較の結果変化が認められなかった場合には401に戻り、次のネットワーク構成検出まで待機する。比較の結果変化が認められた場合、検出された現在のネットワーク構成をセキュアなネットワーク構成の条件と比較し(408)、条件に合致するか否かを判断する(409)。現在のネットワーク構成がセキュアでなネットワーク構成の条件に合致した場合、411に戻り、次のバスリセットが検出されるまで待機する。合致しなかった場合、ユーザに警告を行なう(404)。警告を受けたユーザは現在のネットワーク構成がセキュアであるか否かを判断する。ユーザがセキュアであると判断した場合、現在のネットワーク構成をセキュアなネットワーク構成の条件として新たに登録し(407)、411に戻り、次のバスリセットが検出されるまで待機する。

【0075】なお、ユーザへの警告404は、警告音や音声を利用または表示と警告音、音声を併用した警告を行なってもよい。また、警告理由およびその判断材料となった情報を提示しても良い。また、ネットワークの運用を停止する、ネットワークの接続を強制切断する、等の対策を警告とともに行なっても良い。

【0076】本発明の実施の形態9におけるネットワーク監視方法を以上のように構成することにより、最小の手順でネットワーク構成の変化を検出し、ネットワークに不正な機器の接続された可能性を検出することができ、与えられた条件に因ってネットワークがセキュアか否かを自動的に判断するネットワーク監視方法を実現することができる。

【0077】(実施の形態10)図10は本発明の実施の形態10におけるネットワーク監視装置の構成を示すブロック図であり、図5および図8に示す構成部の符号と同一の符号を有する構成部は同様のため、説明を省略する。

【0078】次に、図10を参照して本発明の実施の形態10におけるネットワーク監視装置の動作を説明する。最初にユーザは、セキュアであると解っているネットワーク構成を許容ネットワーク構成記録部106に登録する。また、ネットワーク構成検出部102は、現在のセキュアなネットワーク構成を検出し、ネットワーク

構成記録部103は、そのネットワーク構成をそれがセキュアであるというセキュリティ情報を付加して記録する。次に、バスリセット検出部109は、ネットワークのバスリセットを検出するとその旨をネットワーク構成検出部102に出力する。ネットワーク構成検出部102は、それを受けてバスリセット後のネットワーク構成を検出する。ネットワーク構成変化検出部104は、現在のネットワーク構成と記録されているセキュアなネットワーク構成とを比較し、ネットワーク構成に変化があった場合それを検出し、判断部107に出力する。また、ネットワーク構成の変化が検出された場合、ネットワーク構成記録部103は、新たなネットワーク構成を、セキュアではないというセキュリティ情報を付加して記録する。判断部107は、ネットワーク構成変化検出部104からの入力を受けると、許容ネットワーク構成記録部106に記録されているセキュアと認定されているネットワーク構成と新たなネットワーク構成とを比較する。もし新たなネットワーク構成が、許容ネットワーク構成記録部106に記録されているセキュアと認定されているネットワーク構成に含まれる場合、判断部107は、ネットワーク構成記録部103に記録された新たなネットワーク構成に付加されたセキュリティ情報を、セキュアであると書き換える。この時、判断部107は、変化があったことを警告発生部108に出力しても良い。もし新たなネットワーク構成が、許容ネットワーク構成記録部106に記録されているセキュアと認定されているネットワーク構成に含まれない場合、判断部107は、その旨を警告発生部108に出力する。警告発生部108は、判断部107からの入力を受け、ユーザに対し警告を発する。ユーザは表示部105を見てそれがセキュアなネットワーク構成であるかどうかを確認し、もしそのネットワーク構成がセキュアであった場合、その旨を入力部110に入力する。ネットワーク構成記録部103は、入力部110からの入力を受け、新たなネットワーク構成に付加されたセキュリティ情報を、セキュアであると書き換える。また、もしそのネットワーク構成がセキュアであった場合、ユーザは入力部110を介して許容ネットワーク構成記録部106に新たなネットワーク構成を追加することもできる。

【0079】なお、警告発生部108は、警告音や音声を利用または表示と警告音、音声を併用した警告を行なってもよい。また、警告理由およびその判断材料となった情報を提示しても良い。また、ネットワークの運用を停止する、ネットワークの接続を強制切断する、等の対策を警告とともに行なっても良い。

【0080】本発明の実施の形態10におけるネットワーク監視装置を以上のように構成することにより、バスリセットにともなうネットワーク構成の変化を最小の手順で検出し、予め与えられた情報を基にネットワークに不正な機器の接続された可能性を自動的に検出できるネ

ットワーク監視装置を実現することができる。

【0081】（実施の形態11）図11は本発明の実施の形態11におけるネットワーク監視装置の構成を示すブロック図である。これは図10の構成において、ネットワーク構成記録部103とネットワーク構成変化検出部104とを省略した構成である。このような構成にした場合、実施の形態10の場合と比較して、ネットワーク構成が変化しない場合でも判断を行わねばならず、判断部107の処理が多くなる一方、全体の構成が簡単になる。

【0082】本発明の実施の形態11におけるネットワーク監視装置を以上のように構成することにより、簡易な構成で、バスリセットにともなうネットワーク構成の変化を最小の手順で検出し、予め与えられた情報を基にネットワークに不正な機器の接続された可能性を自動的に検出できるネットワーク監視装置を実現することができる。

【0083】（実施の形態12）図12は本発明の実施の形態12におけるネットワーク監視方法の流れ図である。421はネットワーク構成検出手段を調査するフェイズ、422は使用できる全てのネットワーク検出手段を用いるフェイズ、423はネットワーク構成を検出するフェイズ、424は検出したネットワーク構成を記録するフェイズ、425は複数の手段から検出されたネットワーク構成に矛盾がないか比較するフェイズ、426はユーザに警告を行なうフェイズである。

【0084】次に図12を参照して、本発明の実施の形態12におけるネットワーク監視方法を説明する。まず最初に、ネットワーク構成を検出する手段としてどのような手段が使用可能かについて調査を行なう（421）。421で得られたネットワーク構成検出手段を用いてネットワーク構成の検出を行なう（422）。各ネットワーク構成検出手段はネットワーク構成を検出し（423）、検出されたネットワーク構成は記録される（424）。なお、ここでは全てのネットワーク構成検出手段を用いることになっているが、指定された数、指定された時間、指定された手段、等実際にネットワーク構成を検出する手段を限定してもよい。検出された複数のネットワーク構成は、互いに矛盾がないか比較される（425）。矛盾が存在した場合、ネットワーク上に不正な機器が存在するか、機器あるいはネットワーク構成検出手段が故障している可能性があるため、ユーザに警告を行なう（426）。矛盾が存在しなかった場合、そのネットワーク構成は正しいものとされ出力される。複数のネットワーク構成検出手段で得られたネットワーク構成に矛盾があった場合、その情報を元に信用できないネットワーク構成検出手段を検出することができる。同様にしてネットワーク構成検出手段の故障を検出することができる。また、ネットワーク構成検出手段を複数持つことで、ネットワーク構成検出手段の故障に対して強靱

となる。

【0085】なお、426でユーザに警告を行なう場合、警告音や音声を利用または表示と警告音、音声を併用した警告を行なってもよい。また、警告理由およびその判断材料となった情報を提示しても良い。また、ネットワークの運用を停止する、ネットワークの接続を強制切断する、等の対策を警告とともに行なってもよい。

【0086】本発明の実施の形態12におけるネットワーク監視方法を以上のように実現することにより、ネットワーク構成獲得手段を複数持つことでフォールトトレランスを維持することができ、また、不正なトポロジマップを検出することでネットワークに不正な機器の接続された可能性を検出できるネットワーク監視方法を実現することができる。

【0087】（実施の形態13）図13は本発明の実施の形態13におけるネットワーク監視装置の構成を示すブロック図であり、図3に示す構成部の符号と同一の符号を有する構成部は同様のため、説明を省略する。図13は図3におけるネットワーク構成検出部102の内部に実現する場合を示しており、102a～102xは複数存在するネットワーク構成検出手段であり、102yは検出されたネットワーク構成を記録する記録部であり、102zは複数の手段から検出されたネットワーク構成に矛盾がないか比較する比較部である。

【0088】次に図13を参照して、本発明における実施の形態13におけるネットワーク監視装置の動作を説明する。ここで説明する実施の形態13は、図3におけるネットワーク構成検出部102の内部に実現する場合について説明する。ネットワーク構成を検出する時刻になる、あるいは検出する指令を受けたネットワーク構成検出部はネットワーク構成の検出を行なう。複数のネットワーク構成検出手段102a～102xは、それぞれの手段でネットワーク構成を検出する。ネットワーク構成を獲得したネットワーク構成検出手段102a～102xは、ネットワーク構成を記録部102yに記録する。比較部102zは、記録部102yに記録された複数の検出手段に因るネットワーク構成を比較し、互いに矛盾がないかを調べる。矛盾が認められなかった場合、ネットワーク構成記録部103とネットワーク構成変化検出部104にネットワーク構成を出力する。矛盾が認められた場合、警告発生部108にその旨を出力する。複数のネットワーク構成検出手段で得られたネットワーク構成に矛盾があった場合、その情報を元に信用できないネットワーク構成検出手段を検出することができる。同様にしてネットワーク構成検出手段の故障を検出することができる。また、ネットワーク構成検出手段102a～102xを複数持つことで、ネットワーク構成検出手段の故障に対して強靱となる。

【0089】本発明の実施の形態13におけるネットワーク監視装置を以上のように構成することにより、ネッ

トワーク構成獲得手段を複数持つことでフォールトトレランスを維持することができ、また、不正なトポロジマップを検出することでネットワークに不正な機器の接続された可能性を検出できるネットワーク監視装置を実現することができる。また、本発明の実施の形態13におけるネットワーク監視装置のように、このネットワーク監視装置を他のネットワーク監視装置のネットワーク構成検出部として実装することも可能であり、それによってセキュリティレベルを上げることができる。

【0090】（実施の形態14）図14は本発明の実施の形態14におけるネットワーク監視方法の流れ図である。431は伝送遅延を測定するフェイズ、432は測定した伝送遅延を記録するフェイズ、433は伝送遅延を比較し、変化を検出するフェイズ、434はユーザに警告を出すフェイズである。

【0091】次に図14を参照して、本発明の実施の形態14におけるネットワーク監視方法を説明する。監視者は設定された時刻にネットワーク上の伝送遅延時間を測定する（431）。測定時刻については、バスリセット直後、一定時間間隔、ランダム時間間隔、トラフィックの少ない時間、特定のイベントの直前または直後、ユーザの指示した時刻、常時、等の手段がある。測定手段としては、遅延測定用のパケットを測定対象ノードに送信しackを観察する、ネットワーク上を流れるリクエストパケットとそれに対するackを観察する、等の手段がある。測定された伝送遅延時間は記録される（432）。新たに記録された伝送遅延時間は、過去に記録された伝送遅延時間、または設定された伝送遅延時間と比較される（433）。比較した結果、伝送遅延時間の変化が認められない場合、431に戻り、次の伝送遅延測定時刻を待つ。伝送遅延の変化が認められる場合、ユーザに警告を行なう（434）。

【0092】なお、434でユーザに警告を行なう場合、警告音や音声を利用または表示と警告音、音声を併用した警告を行なってもよい。また、警告理由およびその判断材料となった情報を提示しても良い。また、ネットワークの運用を停止する、ネットワークの接続を強制切断する、等の対策を警告とともに行なっても良い。

【0093】本発明の実施の形態14におけるネットワーク監視方法を以上のように実現することにより、伝送遅延を計測することができ、伝送遅延の変化からネットワークに不正な機器の接続された可能性を検出できるネットワーク監視方法を実現することができる。また、請求項1～20に記載のネットワーク監視方法およびネットワーク監視装置とともに用いることにより、ネットワークをネットワーク構成とノード間の伝送遅延との二種類の情報から監視することが可能になり、ネットワークのセキュリティレベルを上げることができるという作用を有する。

【0094】（実施の形態15）図15は本発明の実施

の形態15におけるネットワーク監視装置の構成を示すブロック図である。101はネットワーク、121は設定されたネットワーク機器の検出条件を記録する検出条件記録部、123は監視情報を記録しておく記録部、124は記録から伝送遅延の変化を検出する変化検出部、125は変化を検出した場合、警告を発する警告発生部である。126は遅延検査用のパケットを送信するパケット送信部であり、127は遅延検査用のパケットを受信するパケット受信部である。

【0095】図16は検出条件記録部121および記録部123で使用される記録テーブルの概念図である。151は機器毎の検出条件テーブルと応答結果記録テーブルを管理する機器テーブルであり、152は検出条件を記録する検出条件テーブルであり、153はパケットの送信時刻と機器からの応答のパケット受信時刻を記録する応答結果テーブルである。

【0096】次に、図15、16を参照して、本発明の実施の形態15におけるネットワーク監視装置の動作を説明する。最初にユーザは検出条件記録部121に検出条件を設定、記録する。パケット送信部126は、検索条件に従ってネットワーク機器へ遅延測定用のパケットを発信する。パケット受信部127は、機器から返ってきた遅延測定用パケットへの応答を受信する。監視したパケットは記録部123に記録される。変化検出部124は、記録部123の記録と検出条件記録部121の検出条件とから許容されない伝送遅延の変化があるかどうかを検出する。許容されない伝送遅延の変化が検出された場合、警告発生部125はユーザに警告を発する。

【0097】なお、検出条件記録部121に設定、記録される検出条件は、検出時刻、時間、頻度、許容変化範囲、ホップ数、ケーブル長、中継機器などの経路の条件、特殊な機器の条件、機器の秘密共有鍵、機器の公開鍵、送信パケットの条件、機器についての情報などである。また、記録部123は、リクエストのパケットとそれに応じる応答パケットの間の時間を記録しても良く、またパケットのダンプ、パケットの一部、パケットの内容等も併せて記録しても良い。また、警告発生部125は、警告音や音声を利用または表示と警告音、音声を併用した警告を行なってもよい。また、警告理由およびその判断材料となった情報を提示しても良い。また、ネットワークの運用を停止する、ネットワークの接続を強制切断する、等の対策を警告とともに行なっても良い。

【0098】本発明の実施の形態15におけるネットワーク監視装置を以上のように構成することにより伝送遅延を計測することができ、伝送遅延の変化からネットワークに不正な機器の接続された可能性を検出できるネットワーク監視装置を実現することができる。また、請求項1～20に記載のネットワーク監視方法およびネットワーク監視装置とともに用いることにより、ネットワークをネットワーク構成とノード間の伝送遅延との二種類

の情報から監視することが可能になり、ネットワークのセキュリティレベルを上げることができる。

【0099】（実施の形態16）図17は本発明の実施の形態16におけるネットワーク監視装置の構成を示すブロック図である。101はネットワーク、121は設定されたネットワーク機器の検出条件を記録する検出条件記録部、122はネットワーク上のパケットを監視するパケット監視部、123は監視情報を記録しておく記録部、124は記録から伝達遅延の変化を検出する変化検出部、125は変化を検出した場合、警告を発する警告発生部である。

【0100】図18は記録部123で使用する記録テーブルの概念図である。141は機器間経路と応答時間記録テーブルとの関係を記録するテーブルであり、142は機器間の応答時間を記録するテーブルである。

【0101】次に、図17、18を参照して、本発明の実施の形態16におけるネットワーク監視装置の動作を説明する。最初にユーザは検出条件記録部121に検出条件を設定、記録する。パケット監視部122は、検索条件に従ってパケットネットワーク上のパケットを監視し、監視したパケットは記録部123に記録される。図18に示すように、監視は機器間の経路単位で行なわれ、リクエストのパケットとそれに応じる応答パケットの対がそれぞれ観測された時刻が記録される。変化検出部124は、記録部123の記録と検出条件記録部121の検出条件とから許容されない伝達遅延の変化があるかどうかを検出する。許容されない伝達遅延の変化が検出された場合、警告発生部125はユーザに警告を発する。

【0102】なお、検出条件記録部121に設定、記録される検出条件は、検出時刻、時間、頻度、検出するパケット、許容変化範囲、機器間経路のホップ数、ケーブル長、中継機器などの経路の条件、機器とネットワーク監視装置間経路のホップ数、ケーブル長、中継機器などの経路の条件、特殊な機器の条件などである。また、記録部123は、リクエストのパケットとそれに応じる応答パケットの間の時間を記録しても良く、またパケットのダンプ、パケットの一部、パケットの内容等も併せて記録しても良い。また、警告発生部125は、警告音や音声を利用または表示と警告音、音声を併用した警告を行なってもよい。また、警告理由およびその判断材料となった情報を提示しても良い。また、ネットワークの運用を停止する、ネットワークの接続を強制切断する、等の対策を警告とともに行なっても良い。

【0103】本発明の実施の形態16におけるネットワーク監視装置を以上のように構成することにより、ネットワークのトラフィックを増加させることなく簡易な構成で伝送遅延を計測することができ、伝送遅延の変化からネットワークに不正な機器の接続された可能性を検出できるネットワーク監視装置を実現することができる。また、請求項1～20に記載のネットワーク監視方法お

よびネットワーク監視装置とともに用いることにより、ネットワークをネットワーク構成とノード間の伝送遅延との二種類の情報から監視することが可能になり、ネットワークのセキュリティレベルを上げることができる。

【0104】（実施の形態17）図19は本発明の実施の形態17におけるネットワークおよびネットワーク監視装置のふるまいの概念図である。201はネットワーク監視装置であり、202は監視対象のネットワーク機器である。203はネットワークがセキュアであることが確認されたことを示しており、204はネットワークにバスリセットがかかったことを示している。205はバスリセット前に予め交換しておくバスリセット前情報であり、206はバスリセット後に交換される認証情報要求であり、207は認証情報である。

【0105】本発明実施の形態17におけるネットワークに接続されるネットワーク機器は、互いに情報を交換し、交換した情報を記録しておく能力を有する。ネットワーク上の機器はバスリセットが起こる前に予め情報を交換しておき、バスリセット後にその情報を用いることによりバスリセットに因われない運用が可能になる。例えば、バスリセット前に各機器の固有の名前または仮想的なIDと物理IDとの組をバスリセット前に交換しておき、バスリセット後も同様の情報を交換することで、バスリセットの前後で変化する各機器の物理ID変換テーブルを得ることができ、物理IDに因われない運用が可能となり、また、ネットワーク構成の変化も知ることができる。

【0106】次に、図19を参照して本発明の実施の形態17におけるネットワークおよびネットワーク監視装置の動作の例を説明する。ここではバスリセット前に交換した情報をバスリセット後に秘密鍵として用いることで機器の承認を行なう。まず、セキュア確認203を経てネットワークのセキュリティが確認される必要がある。ここでネットワーク上に不正を働くネットワーク機器、悪意を実現することに利用できるネットワーク機器が存在しない状態であることが確認される。セキュアなネットワーク上の情報は秘密情報として扱うことができるため、ネットワーク監視装置201はこの時に鍵となるバスリセット前情報205をネットワーク機器202に送信する。この情報は予測されてはならないため、ここでは乱数を使ったことにする。この乱数を以後乱数Aと呼ぶ。ネットワーク監視装置201およびネットワーク機器202は、このバスリセット前情報205を記憶しておく。

【0107】バスリセット204が起こると、それは新たな機器がネットワークに接続された可能性を示すために、これ以後はネットワークのセキュリティは保証されない。ここでバスリセット前情報205を利用してネットワーク機器202の認証を行なう。ネットワーク監視装置はバスリセット前情報205に含まれる情報、ここ

では乱数Aを関数に通した値を、認証情報要求206と一緒にネットワーク機器202に送信する。ここでは関数としてハッシュ関数を用いている。この関数が、逆変換のできない、あるいは逆変換の困難な方向関数である場合、この関数は公開されていてもよいが、少なくとも相手のネットワーク機器202はこの関数を知っている必要がある。ここではここでは乱数Aを関数に通した値をHash(乱数A)とする。

【0108】認証情報要求を受けたネットワーク機器202は、バスリセット前情報と既知の関数から認証情報要求206に含まれるHash(乱数A)を計算し、ネットワーク監視装置201がバスリセット前情報を交換したネットワーク監視装置であることを確認する。確認後、ネットワーク機器は、乱数Aと自分のIDとのXORをとった値を関数に通した、Hash(乱数A | ID)およびIDを認証情報207としてネットワーク監視装置に送信する。ネットワーク機器が乱数AとIDとのXORをとるのは、認証情報207が認証確認情報206で偽造返してきては困るためであり、既知の異なる関数を用いたり、ネットワーク監視装置201が認証情報要求206と共に塩を送りそれを利用したり、IDの代わりに乱数などの適当な値を用いたりする、などの別の手段を用いてもよい。認証情報207を受信したネットワーク監視装置201は、乱数AとIDからHash(乱数A | ID)を計算し、ネットワーク機器202がバスリセット前情報を交換したネットワーク機器であることを確認できる。このプロセスを全ての機器に行なうことでバスリセット前から接続されていた機器の認証を行なうことができる。このプロセスは、なりすましを防止するために機器毎に行なった方がよい。具体的にはバスリセット前情報205の乱数を機器毎に変えるとよい。

【0109】本発明の実施の形態17におけるネットワークおよびネットワーク監視装置を以上のように構成することにより、バスリセット前に交換した情報をバスリセット後に利用することができるネットワークを得ることができる。また、バスリセット前情報を以上のように利用することで、バスリセット以前から存在する機器の認証を行なうことができるネットワークおよびネットワーク監視装置を得ることができる。

【0110】(実施の形態18)図20は本発明の実施の形態18におけるネットワーク監視装置およびネットワーク機器の構成を示すブロック図である。101はネットワークであり、161はネットワーク監視装置である。ネットワーク監視装置161において、162は送受信部であり、163は機器認証処理を行なう機器認証処理部であり、164は記録部であり、165は鍵生成部であり、166はバスリセット検出部である。171はネットワーク機器であり、172はネットワーク機器の送受信部であり、173はネットワーク機器の機器認

証処理部であり、174はネットワーク機器の記録部である。

【0111】次に、図20を参照して、本発明の実施の形態18におけるネットワーク監視装置およびネットワーク機器の動作を説明する。ネットワークがセキュアであることが確認できた後、ネットワーク監視装置161の鍵生成部165は、認証用の鍵を生成する。鍵は送受信部162を通して伝送され、また伝送先の情報とともに記録部164に記録される。ネットワーク機器171は、送受信部172で鍵を受信し、記録部174に記録する。

【0112】バスリセットが発生すると、バスリセット検出部166がそれを検出し、機器認証処理部163に通知する。機器認証処理部163は、記録部164に記録されている鍵を用いてネットワーク機器の認証のための情報を生成し、送受信部162を通してネットワーク機器171に伝送される。ネットワーク機器171は送受信部172で認証情報を受信する。それを受けて、機器認証処理部173は受信した認証情報および記録部174に記録されている鍵を用いて認証情報を生成し、送受信部172を通してネットワーク監視装置161に送信する。ネットワーク監視装置161の認証処理部163は、送受信部162を介して認証情報を受信し、機器の認証を行なう。

【0113】ここではネットワーク監視装置161がバスリセットを感知し、他のネットワーク機器の認証のトリガとなる情報を生成する例を挙げているが、ネットワーク機器がそれぞれバスリセットを感知し認証情報を生成しても良い。また、ネットワーク機器が鍵を生成しても良い。また、認証を一回の応答で行なっているが、セキュアのために複数回の応答が必要な認証を行なっても良い。なお、バスリセット前の情報として、鍵以外にも、現在のネットワーク構成、次に起こることが想定されるネットワーク構成の変化、などを交換することもできる。

【0114】本発明の実施の形態18におけるネットワーク監視装置およびネットワーク機器を以上のように構成することにより、バスリセット前に交換した情報をバスリセット後に利用することができるネットワーク監視装置およびネットワーク機器を得ることができる。また、バスリセット前情報を以上のように利用することで、バスリセット以前から存在する機器の認証を行なうことができるネットワーク監視装置およびネットワーク機器を得ることができる。

【0115】(実施の形態19)図21は本発明の実施の形態19における監視システムの構成例を示すブロック図である。301はカメラ、302はマイク、303はセンサ、304は表示装置、305は記録装置、306はバスブリッジ、307はユーザ端末、308は請求項1~26に記載のネットワーク監視方法を具備した機

器あるいはネットワーク監視装置である。

【0116】次に、図21を参照して本発明の実施の形態19における監視システムの動作を説明する。最初にユーザはユーザ端末307から設定項目をネットワーク監視装置308に入力する。次にネットワーク監視装置308は、ネットワーク構成情報を取得し、ネットワーク構成が許容されているものであるかどうかを判断し、許容されていない場合にはユーザに警告を行なう。また、ネットワーク監視装置308は、ネットワーク上の伝送遅延を調査し、伝送遅延の変化が許容されているものかどうかを判断し、許容されていない場合にはユーザに警告を行なう。また、ネットワークが許容される状態である時はセキュアであると判断し、ネットワーク監視装置308は、予め秘密鍵となる情報をネットワーク機器301～306と交換しておく。バスリセットの発生は、ネットワーク構成の変化の可能性を意味するため、少なくともバスリセット毎にネットワーク監視装置308はネットワーク構成および伝送遅延を取得し、許容されているものであるかどうかを調査する。

【0117】警告が出された場合、それはネットワークが設定で許されていない状態に変化したことを意味する。ユーザは警告を受け、現在の状態を警告に付随する情報を利用して調査を行なう。その結果、その状態もセキュアであるとユーザが判断した場合、ユーザ端末307を通してその旨をネットワーク監視装置308に伝える。ネットワーク監視装置308はその状態を許容される状態として蓄積する。

【0118】本発明の実施の形態19における監視システムを以上のように構成することにより、ネットワークに接続しようとする不正な機器を発見し、ネットワークをセキュアに保つことができるネットワーク監視システムを得ることができる。

【0119】

【発明の効果】以上のように、本発明によれば、ネットワーク構成を監視することにより、ネットワークへの機器の追加、削除およびネットワーク構成の変化を検出し、ネットワークへの不正な機器の接続を発見することができるネットワーク監視装置を得ることができる。また、伝送遅延を監視することによりネットワークへの機器の追加、削除およびネットワーク構成の変化を検出し、ネットワークへの不正な機器の接続を発見することができるネットワーク監視装置を得ることができる。また、バスリセット前に情報を交換しておくことによりバスリセット前から接続されている機器の認証を行ない、ネットワークへの機器の追加、削除およびネットワーク構成の変化を検出し、ネットワークへの不正な機器の接続を発見することができるネットワーク監視装置を得ることができる。また、ネットワーク自体をセキュアに保つことのできるネットワーク監視システムを得ることができる。

【図面の簡単な説明】

【図1】本発明の実施の形態1におけるネットワーク監視方法を説明する概念図

【図2】本発明の実施の形態2におけるネットワーク監視方法の構成を示す流れ図

【図3】本発明の実施の形態3におけるネットワーク監視装置の構成を示すブロック図

【図4】本発明の実施の形態4におけるネットワーク監視方法の構成を示す流れ図

【図5】本発明の実施の形態5におけるネットワーク監視装置の構成を示すブロック図

【図6】本発明の実施の形態6におけるネットワーク監視装置の構成を示すブロック図

【図7】本発明の実施の形態7におけるネットワーク監視方法の構成を示す流れ図

【図8】本発明の実施の形態8におけるネットワーク監視装置の構成を示すブロック図

【図9】本発明の実施の形態9におけるネットワーク監視方法の構成を示す流れ図

【図10】本発明の実施の形態10におけるネットワーク監視装置の構成を示すブロック図

【図11】本発明の実施の形態11におけるネットワーク監視装置の構成を示すブロック図

【図12】本発明の実施の形態12におけるネットワーク監視方法の構成を示す流れ図

【図13】本発明の実施の形態13におけるネットワーク監視装置の構成を示すブロック図

【図14】本発明の実施の形態14におけるネットワーク監視方法の構成を示す流れ図

【図15】本発明の実施の形態15におけるネットワーク監視装置の構成を示すブロック図

【図16】本発明の実施の形態15におけるネットワーク監視装置の監視記録テーブルの概念図

【図17】本発明の実施の形態16におけるネットワーク監視装置の構成を示すブロック図

【図18】本発明の実施の形態16におけるネットワーク監視装置の監視条件、記録テーブルの概念図

【図19】本発明の実施の形態17におけるネットワーク監視方法の概念図

【図20】本発明の実施の形態18におけるネットワーク監視装置のブロック図

【図21】本発明の実施の形態19における監視システムの概念図

【符号の説明】

101 ネットワーク

102 ネットワーク構成検出部

102a～102x ネットワーク構成検出手段

102y 記録部

102z 比較部

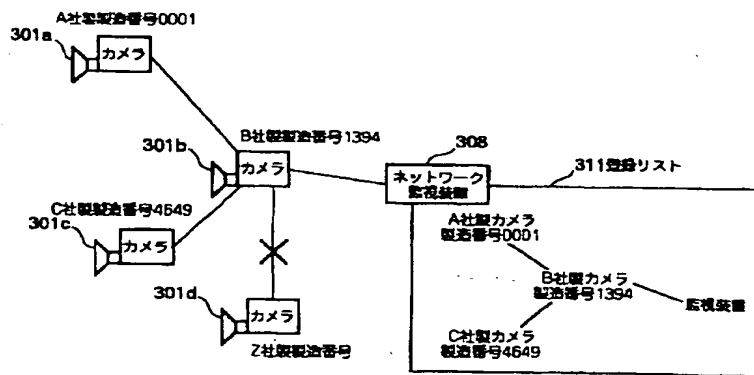
103 ネットワーク構成記録部



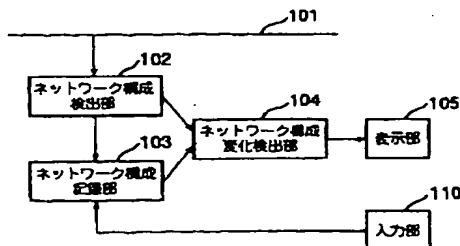
104 ネットワーク構成変化検出部  
 105 表示部  
 106 許容ネットワーク構成記録部  
 107 判断部  
 108 警告発生部  
 109 バスリセット検出部  
 110 入力部  
 121 検出条件記録部  
 122 バケット監視部  
 123 記録部  
 124 変化検出部  
 125 警告発生部  
 126 バケット送信部  
 127 バケット受信部  
 141 経路テーブル  
 142 応答時間記録テーブル  
 151 機器確認テーブル  
 152 検出条件テーブル  
 153 応答結果記録テーブル  
 161 ネットワーク監視装置  
 162 送受信部  
 163 機器認証処理部  
 164 記録部

165 鍵生成部  
 166 バスリセット検出部  
 171 ネットワーク機器  
 172 送受信部  
 173 機器認証処理部  
 174 記録部  
 201 ネットワーク監視装置  
 202 ネットワーク機器  
 203 セキュア確認  
 204 バスリセット  
 205 バスリセット前情報  
 206 認証情報要求  
 207 認証情報  
 301 カメラ  
 302 マイク  
 303 センサ  
 304 表示装置  
 305 記録装置  
 306 バスブリッジ  
 307 ユーザ端末  
 308 ネットワーク監視装置  
 311 登録リスト

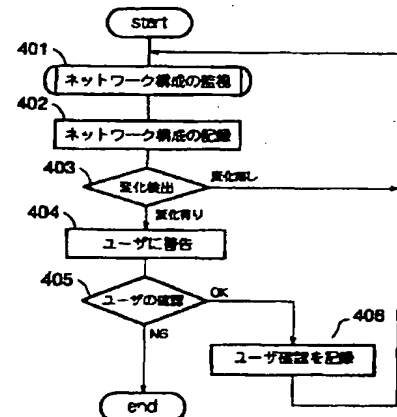
【図1】



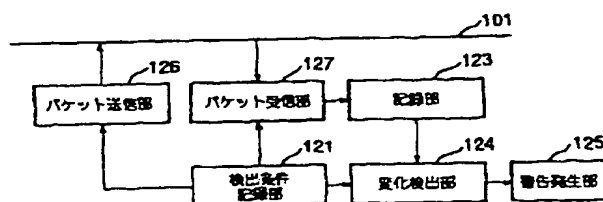
【図3】



【図2】

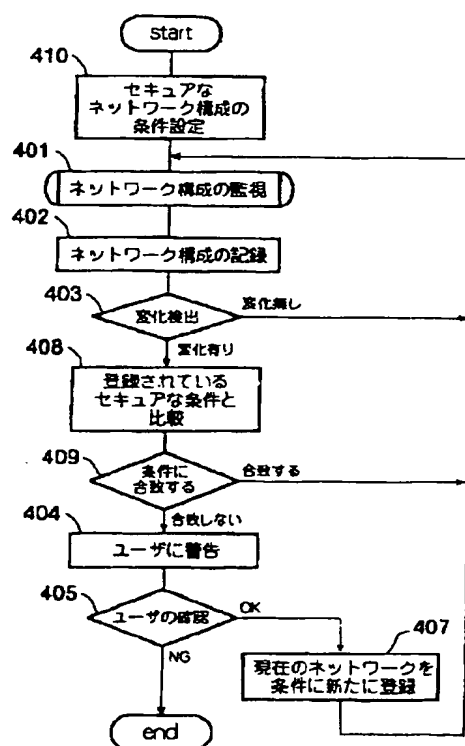


【図15】

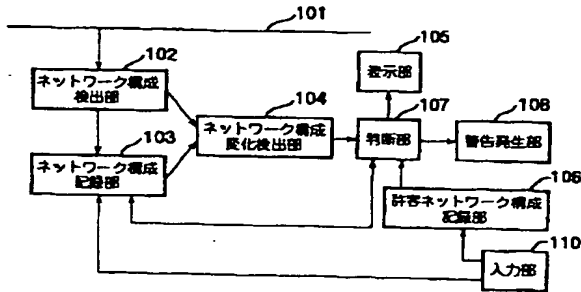


【図4】

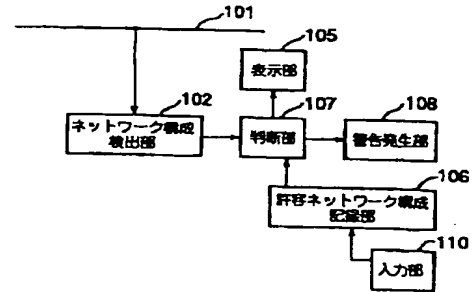
110053-4



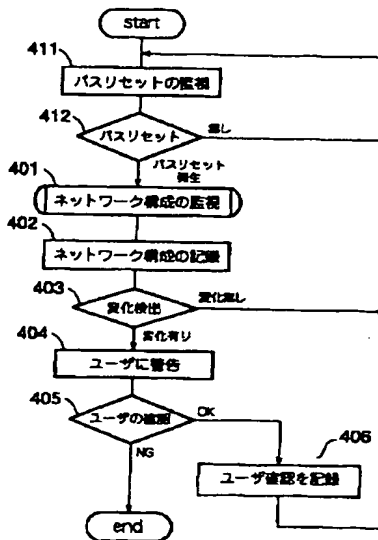
【図5】



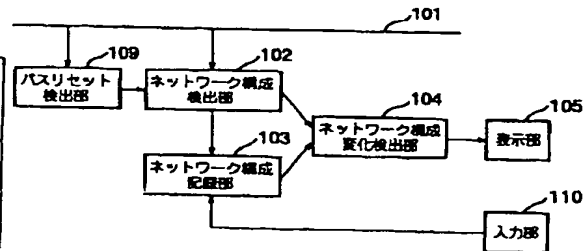
【図6】



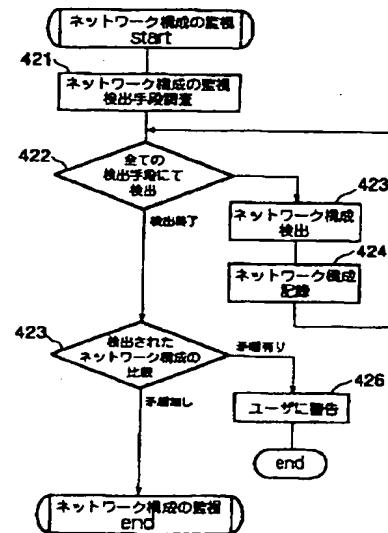
【図7】



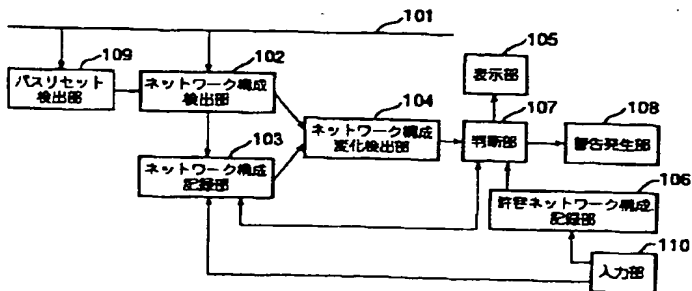
【図8】



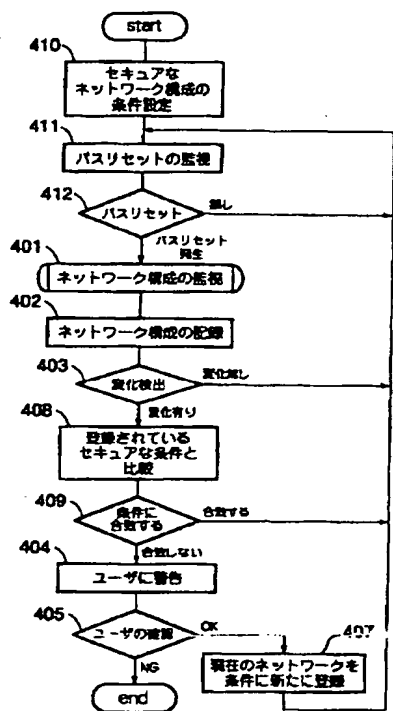
【図12】



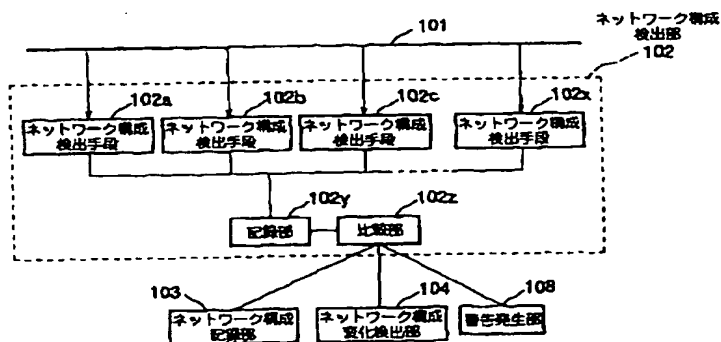
【図10】



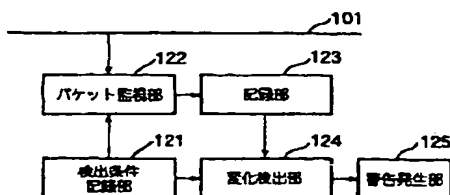
【図9】



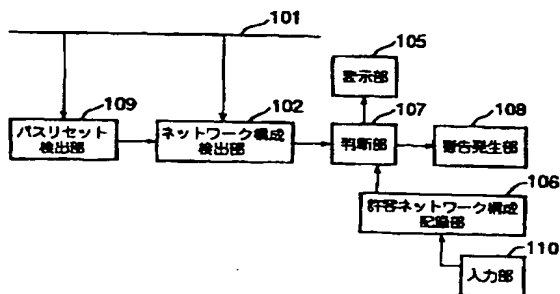
【図13】



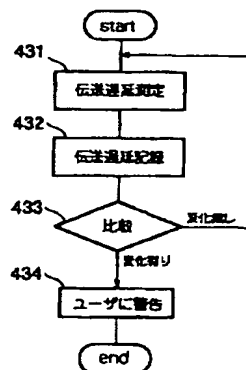
【図17】



【図11】



【図14】



【図18】

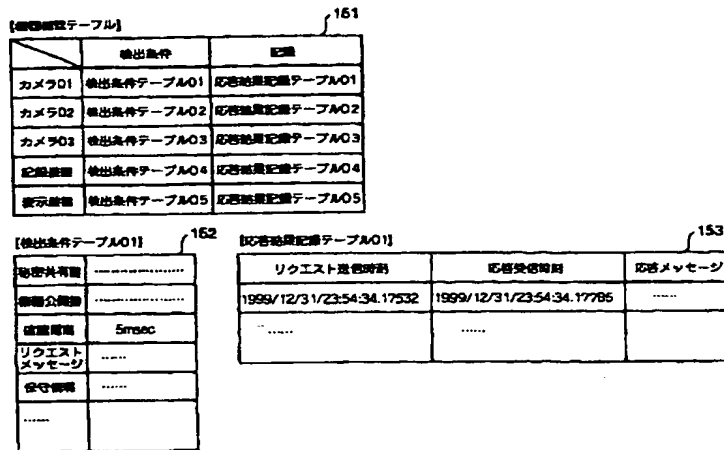
(監視テーブル)

	カメラ01	カメラ02	カメラ03	----
カメラ01	テーブル11	テーブル12	テーブル13	----
カメラ02	テーブル21	テーブル22	-----	
カメラ03	テーブル31	テーブル32	-----	
監視装置	テーブル41	-----		
記録装置	テーブル51	-----		
監視装置	テーブル61	-----		

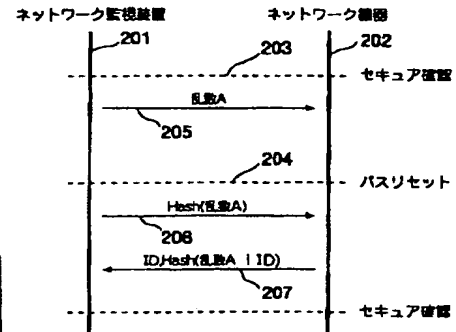
【応答時間記録テーブル1】

リクエスト番号	応答時間
カメラ01	記録装置
リクエスト受信時刻	応答受信時刻
2001/01/08/18:30:12.57246	2001/01/08/18:30:12.57452
2001/01/08/18:30:17.23284	2001/01/08/18:30:17.23418
.....	.....

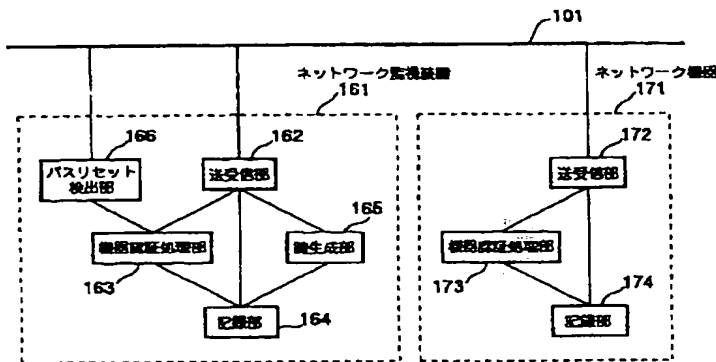
【図16】



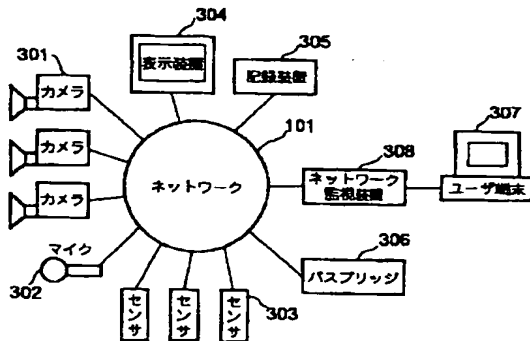
【図19】



【図20】



【図21】



フロントページの続き

(72)発明者 都築 健吾  
神奈川県横浜市港北区綱島東四丁目3番1  
号 松下通信工業株式会社内

Fターム(参考) SK030 GA15 HB08 HC13 JT04 MA01  
MA06 MD07 MD08  
SK033 AA08 BA01 BA08 DA01 DA16  
DB20 EA03